

REMARKS

The requested amendments are necessitated by typographical errors and revisions to figure numbers and reference numbers necessitated by changes made in the formal drawings which are transmitted herewith. There is no new matter introduced as a result of these amendments.

If there are any fees due in connection with the filing of this paper, please charge the fees to our Deposit Account No. **50-0310**. A duplicate copy of this page is enclosed. The Examiner is invited to contact the undersigned at 215-963-5091 to discuss any matter concerning this application.

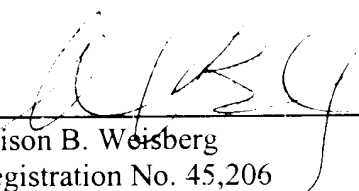
Respectfully submitted,

MORGAN, LEWIS & BOCKIUS, LLP

Dated: _____

3/19/03

By: _____


Alison B. Weisberg
Registration No. 45,206
1701 Market Street
Philadelphia, PA 19103
(215) 963-5000

VERSION WITH MARKINGS TO SHOW CHANGES TO SPECIFICATION

[0020] ~~[Figure 8 is a]~~**Figures 8A-8B are** flow ~~[chart]~~**charts** illustrating a method for storing and selectively sharing end-user information in accordance with a preferred embodiment of the present invention.

[0028] End users 500, platform 100, and providers 600 may connect to each other through a variety of different types of links to form a network~~[-2000-]~~. For example, end users 500 may connect to platform 100 through the Internet 50, directly through link 51 and link 52, or by way of provider 600, though link 51, link 53 and link 54. In other embodiments, alternate configurations of the connections between end users 500, platform 100 and providers 600 are possible, will be known to those skilled in the art and are within the scope of the present invention. In some embodiments, one or more of the links between these various entities is wireless.

[0030] The administrative relationship between access providers and services providers can be described with reference to Figure 1B. An access provider may establish an operational account 1195 within platform 100 (using code catalog component 109 shown in and discussed with reference to Figure 2A). Similarly, a service provider may establish an operational account 1196 within platform 100. Each end user 500 present on the network 2000 within system 1000 is sponsored by at least one access provider. Each access provider "owns" each end user 500 it sponsors in that such access provider has the sole authority to permanently discontinue the access of the end user 500 it sponsors to **the** network~~[-2000-]~~. Similarly, an access provider may supply to end users 500, and thus own, certain devices 20. On the other hand, a service provider may own particular types of private codes 1098 upon which its services 1097 may operate. Its services 1097 may

also operate on public codes 1099. Services 1097 of the service provider may be enabled for particular types of contexts 1180, or may be limited by these contexts 1180, as discussed below in more detail with reference to Figure 2A. In the preferred embodiment, a single organization may serve as both a service provider and an access provider.

[0032] Figure 2A illustrates a further preferred embodiment, including more detail, of the system 1000 shown in Figure 1A. With reference to both Figures 1A and 2A, services/applications 650 represent services and applications offered within system 1000 by providers 600 and provide value to end users 500. Exemplary services/applications 650 shown in Figure 2A include shopping services, including grocery shopping services, and publishing and content management services. However, any type of web service/application 650 could be offered through system 1000 within the scope of the present invention. As described previously with reference to Figure [1]2A, end users 500 may employ a variety of devices 550 to communicate information to and receive information from system 1000.

[0035] Session service 130 of platform 100 ensures continued user connection and authentication within a single application sign on. End users 500 using system 1000 navigate across disparate systems owned and run by different organizations and, thus, session service 130 is provided to ensure that the experience of the end user 500 is contiguous. Session service 130 defines the parameters passed from/to external services 650 to/from the platform 100 as an end user 500 passes from one to the other. These parameters may include the following: service identification; the end user identifier (e.g., the GUID described in more detail below); session echo data (i.e., information that the

platform 100 has indicated ~~[+]~~it wants back from the external service 650 when the user returns to the platform 100); external echo data (i.e., information the external service 650 has indicated it wants from the platform 100 when the end user returns to the external service 650); a ticket associated with a list of codes; a time stamp; and a digest that is computed based on the values of the foregoing parameters.

[0053] Figure 4C illustrates the manner in which folders 217, associated with a particular GUID 1055, comprise groups of codes 218, which have both BLOBs 2181 and annotations 2182 associated with them. This information (i.e., the group of codes associated with each GUID and its associated BLOBs 2181 and annotations 2182) is saved in scan cache component ~~[+07]~~107. Thus, the value added by a user in making an annotation to the list (e.g., taking a grocery list and creating a recipe by adding quantities associated with each grocery item) or applying a service 650 to the list, along with the BLOB, is preserved across all interactions for that end user 500 for the particular service provider. This value can then be passed along to others by the end user 500, for example, by emailing the recipe to another user. The other user may not previously have been sponsored on the network~~[-2000-]~~₁, but may become so upon receiving the recipe. Thus, a further commercial advantage is obtained.

[0054] Returning again to Figure 2A and a description of the components of platform 100, code profile component 108 stores information about codes and the services associated with the codes. In general, the filtering functionality of platform 100 uses code profile component 108 to take a series of codes (inputted by an end user 500 through scanning or other inputting techniques) and turn the codes into actions. In particular, code profile component 108 uses active operational mapping from a code

inputted by an end user 500, profile information of the end user 500 (including preferences and any services to which the end user 500 has subscribed) from directory component 105; device profile information of the device used to input the code (including ownership information and any restrictions placed on usage) from directory component 105; and context information (i.e., property information of a session of the end user 500 on the network[~~-2000~~]) to return to the end user 500 pointers to specific services/applications 650.

[0069] Figure 7 provides an example of a preferred embodiment of a system 7000 that may be used to implement the methods of the present invention. Calls made by end users 500 through the end user GUI 210 (described with reference to Figure 2A, for example) may be satisfied by consumer zones ~~[710,]~~711, each of which includes web servers ~~[711]~~713 and application servers ~~[712,]~~710. Each consumer zone ~~[710]~~711 also includes fire walls ~~[713,]~~712. While this exemplary embodiment depicts three consumer zones ~~[710,]~~711, any number of consumer zones may be employed, as needed, in accordance with the present invention. Thus, system ~~[700]~~7000 is scalable. Administrative segment 720 satisfies calls made through account manager 230 and code manager 220, as described with reference to Figure 2A. Authentication of end users may also be carried out through authentication service 721 of administrative segment 720. Statement of record area 730 provides back up of all the information maintained on platform 100 (described with reference to Figure 2A) and, thus, should be highly secure. Internet access to system 7000 can be achieved through internet connection segment 740.

[0070] With reference to ~~[Figure 8,]~~**Figures 8A and 8B**, a method for storing and selectively sharing end-user information, in a system having a plurality of end-users that

remotely access a network having at least a hub site and a plurality of provider sites, is illustrated. In step 801, a user-record corresponding to each end user is stored in a profile database associated with the hub site. Each user-record comprises public information that the end-user submits to the hub site and that the end-user expects will be shared with one or more of the providers without permission of the end-user, private information that the end-user submits to the hub site and that the end-user expects will not be shared with any of the providers without permission of the end-user, and a non-externally identifying symbol associated with the user-record that identifies the end-user on the network. In step 802, a first request signal containing the non-externally identifying symbol corresponding to the end-user is received. In step 803, the public information associated with the end-user is transmitted, in response to the first request signal, from the hub site to a provider without permission of the end-user. In step 804, a second request signal containing the non-externally identifying symbol corresponding to the end-user is received. In step 805, a permission request is transmitted from the hub site to the end-user. In step 806, it is determined if permission of the end-user is received in response to the permission request. If so, in step 807, the private information associated with the end-user is transmitted from the hub site to the provider. If not, in step 808, the private information is not transmitted.

[0071] In some embodiments, each user-record further includes financial information associated with the end-user. In this embodiment, in step 809, a third request signal containing the non-externally identifying symbol corresponding to the end-user is received. In step 810, a second permission request is transmitted in response to the third request signal from the hub site to the end user. In step 811, it is determined whether

permission of the end-user is received in response to the second permission request. If not, in step 812, the financial information is not transmitted. ~~[If so]~~ **As shown in Figure 8B, if permission is received**, in step 813, it is determined whether authentication information from the provider is received. If so, in step 814, the financial information associated with the end-user is transmitted from the hub site to the provider. If not, in step 820 the financial information is not transmitted.

[0072] In other embodiments, each user-record further includes provider preference information associated with the end-user. ~~[If so]~~ **As shown in Figure 8A, in** these embodiments, in step 815, a fourth request signal containing the non-externally identifying symbol corresponding to the end-user is received. In step 816, in response to the fourth request signal, a third permission request is transmitted from the hub site to the end user. In step 817, it is determined if permission of the end-user is received in response to the third permission request. If not, in step 818, the provider preference information is not transmitted. If so, in step 819, the provider preference information associated with the end-user is transmitted from the hub site to the provider.

[0073] With reference to Figure 9, in a system having a plurality of end-users that remotely access a network having at least a hub site and a plurality of provider sites, a method of identifying for at least one of the end-users a location on the network of at least one of the providers is illustrated. In step 901, code information corresponding to one or more codes (e.g., machine readable codes) provided by the end-user (e.g., by scanning) is received at the hub site. In step 902, in response to the code information, network address information corresponding to the location on the network of a provider that is associated with the received code information is retrieved from a profile database

associated with the hub site. In step 903, the network address information is used to direct the end-user to the location on the network of the associated provider. The profile database includes a user-record corresponding to each end user. ~~[the]~~The user-record includes public information that the end-user submits to the hub site and that the end-user expects will be shared with one or more of the providers without permission of the end-user, private information that the end-user submits to the hub site and that the end-user expects will not be shared with any of the providers without permission of the end-user, and a non-externally identifying symbol associated with the user-record that identifies the end-user on the network.